

# NATIONAL INSTITUTE OF TECHNOLOGY PATNA

## Department of Computer Science and Engineering

### Assignment 2

Program: B. Tech. in Computer Science and Engineering

Course Title: Information Security, Credit: 3

---

#### ***Instructions:***

- 1. KEEP YOU COPY CLEAN. HIGHLIGHT/ UNDERLINE THE KEY PARTS.***
  - 2. Type your answer on MS Word only and submit the DOCX file Only***
  - 3. Assignment length must be minimum 3000 words***
  - 4. Don't simply copy the text from other sources. Plagiarism will be checked with professional tool.***
- 

Company's information is extremely important, and writing an information security policy is paramount to keeping it secure. You will need to figure out how management views security, get a good framework, and then adapt it to the company. Decide on your mandates, sub-policies, and supplementary documents. Then you can design a policy with all the crucial elements, taking great care when writing and editing to ensure it is strong. The Security Policy is used to change and support the behavior of a computer system as well as users. The security compliance and standards you must keep in mind. The policy document must contain the following:

- Compiled report with detail of issues by analyzing security risks and their impacts on business
  - Account Policies
    - Password Policy
    - Account Lockout Policy
  - Local Policies Include
    - Audit Policy
    - User rights Assignment Policy
    - Security Options
  - Compiled report with recommendations for the hypothetical company
  - Configure firewall and provide configuration against three types of attack
1. Develop an "Information Security Policy" for a Bank in order to always get the trust of society including our customers by taking drastic and high-level measures against the risk of information leakage to comply with "Information Security Policy" and "Personal Information Protection Principles (privacy policy)" as separately and maintain information security by protecting information assets from various threats and by properly handling them. (Roll No. 1 to 10 and Roll No. 191 to rest)
  2. Implementing an Information and Communications Technology (ICT) systems security policy (Roll No. 11 to 20 and Roll No. 121-130)

3. Write a 2000 words report on NIST 800-100 NIST 800-12 Technical Access Control AC-2 Account Management P1.(Roll No. 21 to 30)
4. Security Policies for cloud access security and cloud security center (Roll No. 31 to 40)
5. General Security Policy for a e-commerce company(Roll No. 41 to 50)
6. Network Security Policy for a cable TV company(Roll No. 51 to 60)
7. Server Security Policy for a data analytic company(Roll No. 61 to 70)
8. Software Installation Policy and Application Security Policy for a travel management company(Roll No. 71 to 80)
9. Workstation Security for HIPAA Policy(Roll No. 81 to 90)
10. Wireless Communications Security Policy(Roll No. 91 to 100)
11. Web Application Security Policy(Roll No. 101 to 110)
12. Security Response Plan Policy(Roll No. 111 to 121)
13. Email Policy, Password Protection Policy, Remote Access Policy(Roll No. 131 to 140)
14. Data Breach Response Policy and Disaster Recovery Plan Policy(Roll No. 141 to 150)
15. Process network security and Firewall configuration policy(Roll No. 151 to 160)
16. Data protection policy(Roll No. 161 to 170)
17. Information security indecent management policy(Roll No. 171 to 180)